

Security Scan Report

Scan Information

Target:	bennett.edu.in
Scan ID:	24f2a26d-0174-419b-ac98-b896c61fa70c
Date:	2025-04-28 03:52:41
Status:	N/A

Vulnerability Summary

Severity	Count
High	6
Medium	5
Low	3
Informational	3

Scan Results

Nmap Scan Results

Port	Protocol	State	Service	Product	Version
80	tcp	open	http-proxyF5 BIG-IP load balancer http proxy		N/A
443	tcp	open	http	Apache httpd	N/A

Web Vulnerabilities

ID	Severity	Description
Target Host	Informational	bennett.edu.in
Target Port	Informational	80
GET /	Informational	The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options :

GET /	Medium	The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/ :
-------	--------	---

CVE Details

CVE ID	Severity	CVSS Score	Description
CVE-2022-6366	LOW	5.0	Vulnerability in F5 BIG-IP load balancer http proxy allows attackers to perform information disclosure via
CVE-2024-9089	HIGH	9.8	Vulnerability in F5 BIG-IP load balancer http proxy allows attackers to perform authentication bypass via
CVE-2024-1303	LOW	5.0	Vulnerability in F5 BIG-IP load balancer http proxy allows attackers to perform information disclosure via
CVE-1999-0236	HIGH	7.5	ScriptAlias directive in NCSA and Apache httpd allowed attackers to read CGI programs.
CVE-1999-0071	High	7.5	Apache httpd cookie buffer overflow for versions 1.1.1 and earlier.
CVE-2001-0206	Medium	5.0	Vulnerability in Apache httpd before 1.3.11, when configured for mass virtual hosting using mod_rewrite, or mod_vhost_alias in Apache 1.3.
CVE-2002-1850	HIGH	7.5	Apache httpd 2.0.40 allows local users to perform remote attacks to cause a denial of service (hang and memory consumption) by causing a CGI script to send a large
CVE-2003-0249	High	7.5	NOTE: CVE-2003-0249 has been disputed by the Apache security team, saying "It is by design that PHP allows scripts to process any request
CVE-2004-0098	Medium	6.4	Apache httpd 2.0.40 allows remote attackers to cause a denial of service (memory exhaustion), and possibly an integer signedness error leading to a heap
CVE-2004-2343	High	7.2	identified in httpd.conf which such as Deny From All, by using an ErrorDocument directive. NOTE: the vendor has disputed this issue, since the .htacce
CVE-2005-1352	Medium	4.3	On CVE-2005-1352, mod_include of Apache httpd before 1.3.35-dev and Apache httpd 2.0.x before 2.0.56-dev allows remote attackers to
CVE-2005-2838	Medium	5.0	On CVE-2005-2838, users to obtain sensitive information, such as the password from adm.conf via an IFRAME element, probably involving an
CVE-2004-0625	Low	3.0	On CVE-2004-0625, local users to bypass certain Apache HTTP Server httpd.conf options, such as safe_mode and open_basedir, via the ini

Recommendations

- Keep all software up-to-date with the latest security patches
- Implement proper network segmentation to limit access to sensitive systems
- Use strong password policies and consider multi-factor authentication
- Monitor system logs for suspicious activities
- Regularly perform security scans and penetration testing
- Follow the principle of least privilege for user access